Deutscher Bundestag **Drucksache 17/5560**

17. Wahlperiode 13. 04. 2011

Kleine Anfrage

der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, Ulla Jelpke, Jens Petermann, Kathrin Senger-Schäfer, Raju Sharma, Frank Tempel, Halina Wawzyniak und der Fraktion DIE LINKE.

Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität – Das Nationale Cyber-Abwehrzentrum

Am 23. Februar 2011 machte das Bundesministerium des Innern (BMI) über eine Pressemitteilung bekannt, dass das Bundeskabinett eine neue Cyber-Sicherheitsstrategie beschlossen habe:

„Ziel der Strategie ist, Cyber-Sicherheit in Deutschland auf einem hohen Niveau zu gewährleisten – ohne dabei die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen. Kernpunkte der neuen Strategie sind:

– der verstärkte Schutz Kritischer Infrastrukturen vor IT-Angriffen,

– der Schutz der IT-Systeme in Deutschland einschließlich einer Sensibilisierung der Bürgerinnen und Bürger,

– der Aufbau eines Nationalen Cyber-Abwehrzentrums ab 01. April 2011 sowie die Einrichtung eines Nationalen Cyber-Sicherheitsrates.“

Weiter heißt es in der Pressemitteilung des BMI:

„Das Nationale Cyber-Abwehrzentrum wird unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) errichtet. Direkt beteiligt werden das Bundesamt für Verfassungsschutz, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Weitere Behörden werden mitwirken. Die Aufgabe des Cyber-Abwehrzentrums besteht darin, Informationen auszutauschen. Das Nationale Cyber-Abwehrzentrum ermöglicht es, schnell und abgestimmt alle Informationen zu Schwachstellen in IT-Produkten oder IT-Vorfällen zu vernetzen, diese zu analysieren und Empfehlungen zum Schutz der IT-Systeme zur Verfügung zu stellen bzw. auszusprechen. Koordiniert wird die Arbeit im Rahmen der Cyber-Sicherheitsstrategie durch den neu einzurichtenden Cyber-Sicherheitsrat unter der Verantwortung der Beauftragten der Bundesregierung für Informationstechnik.“ (Pressemitteilung des BMI vom 23. Februar 2011).

Auch auf internationaler Ebene, hier vor allem auf der EU-Ebene und in der NATO wird von bundesdeutschen Sicherheitsbehörden seit Jahren eine enge Kooperation angestrebt.

So führte im November 2010 die 2004 gegründete Europäische Agentur für Netz- und Informationssicherheit (ENISA, European Network and Information Security Agency) ein erstes europaweites Manöver durch. Der Schlussbericht dazu liegt noch nicht vor.

Wir fragen die Bundesregierung:

1. Welche genauen tatsächlichen Sachverhalte und Vorkommnisse sowie eventuell offenbar gewordenen Schwächen in der bisherigen Arbeit der Sicherheitsbehörden haben dazu geführt, dass ein Nationales Cyber-Abwehrzentrum am 1. April 2011 seine Arbeit aufnehmen soll (bitte für die einzelnen Behörden, Gremien und Kooperationseinrichtungen gesondert darstellen)?
2. Auf welcher gesetzlichen Grundlage soll dieses Nationale Cyber-Abwehrzentrum arbeiten, und ist hierfür – nach Ansicht der Bundesregierung – ein eigenes Errichtungsgesetz oder eine Errichtungsanordnung (falls vorhanden bitte der Antwort beifügen) erforderlich, und wenn nein, warum nicht?
3. Aufgrund welcher sonstigen Verwaltungsvereinbarung wurde das Nationale Cyber-Abwehrzentrum dann errichtet (die Dokumente, Vereinbarungen etc. bitte der Antwort beifügen)?
4. Welche Behörden sollen in dem Nationalen Cyber-Abwehrzentrum mit wie vielen Personen ständig arbeiten, und welche Ad-hoc-Assoziationen sind denkbar?
5. Wie ist die Kooperation der unterschiedlichen Behörden im Nationalen Cyber-Abwehrzentrum konkret geregelt (bitte eventuelle Kooperationsvereinbarungen der Antwort beilegen)?
6. Wie sollen die Arbeit und die Arbeitsabläufe des Zentrums konkret aussehen?
7. Wie bewertet die Bundesregierung die verfassungsrechtlichen Probleme der dauerhaften analytischen und operativen Zusammenarbeit zwischen Bundeskriminalamt (BKA), Bundespolizei, Bundesamt für Verfassungsschutz, Bundesnachrichtendienst (BND), Bundeswehr, Militärischem Abschirmdienst (MAD) und anderen Behörden?
8. Welche Vorsorge ist in den Verwaltungsvereinbarungen getroffen, um den Persönlichkeitsschutz, die Meinungsfreiheit, das Recht auf informationelle Selbstbestimmung der Internetnutzer zu schützen?
9. Sind Informationspflichten gegenüber den von Recherchen betroffenen Nutzern des Internets vorgesehen, wenn ja, wie sehen die aus, und wenn nein, warum nicht?
10. Welche Deliktgruppen der IuK-Kriminalität (IuK: Informations- und Kommunikationstechnik) werden bzw. sollen im Nationalen Cyber-Abwehrzentrum untersucht werden, und gibt es besondere Deliktgruppen der IuK-Kriminalität, die im Nationalen Cyber-Abwehrzentrum ausdrücklich nicht untersucht und bekämpft werden sollen?

    Wenn ja, aus welchen Gründen sind ihre Untersuchung und Bekämpfung nicht vorgesehen?
11. Welche Schwachstellen bei welchen IT-Produkten und bei welchen IT-Vorfällen sollen im Nationalen Cyber-Abwehrzentrum untersucht werden, und besteht das Nationale Cyber-Abwehrzentrum darauf, von den Software-Firmen über sogenannte Backdoors, das heißt absichtlich implementierte Sicherheitslücken, informiert zu werden?
12. Wie wird sich die Zusammenarbeit des Nationalen Cyber-Abwehrzentrums mit dem Bundesministerium für Wirtschaft und Technologie gestalten, und welchen Anteil hatte dieses Bundesministerium an der Entwicklung des Konzepts und der Umsetzung des Nationalen Cyber-Abwehrzentrums?
13. Wie soll die Zusammenarbeit zwischen dem Nationalen Cyber-Abwehrzentrum und den Organisationen und Verbänden der Wirtschaft gestaltet wer-

den, wie z. B. dem BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., dem Bundesverband der Deutschen Industrie e. V. und anderen?

14. In welchen Räumlichkeiten bei welcher Sicherheitsbehörde soll das Nationale Cyber-Abwehrzentrum zukünftig untergebracht werden?

15. Wird das Nationale Cyber-Abwehrzentrum über eine eigene Datei verfügen, und welche nationalen und internationalen Behörden sollen hierauf welche Art von Zugriff (schreibend, lesend, automatisiert – bitte auflisten) haben können?

16. Wem sollen die im Nationalen Cyber-Abwehrzentrum erstellten Lagebilder zur Verfügung gestellt werden, und wer sind die Aufsichtsbehörden der kritischen Infrastrukturen (bitte auflisten), und wie soll die Kooperation mit diesen im Nationalen Cyber-Abwehrzentrum aussehen?

17. Welche genauen Aufgaben (bitte die genaue Aufgabenbeschreibung der Antwort beifügen) hat bzw. soll der Nationale Cyber-Sicherheitsrat im Rahmen seiner koordinierenden Tätigkeit wahrnehmen, und welche interne Organisationsstruktur (vergleiche z. B. Gemeinsames Terrorismusabwehrzentrum – GTAZ) wird sich der Nationale Cyber-Sicherheitsrat geben?

18. Welche genauen Regelungen und Vereinbarungen gibt es für die Tätigkeit des Nationalen Cyber-Sicherheitsrates (bitte der Antwort beifügen)?

19. Wie vereinbart die Bundesregierung den Vorsitz im Nationalen Cyber-Sicherheitsrat durch die Bundesbeauftragte der Bundesregierung für Informationstechnik, wenn deren Aufgaben bisher sind, „den Service der Verwaltung zu verbessern, Innovationen zu fördern, administrative Handlungsfähigkeit zu bewahren sowie die Effizienz in der Verwaltung zu steigern. Diese Ziele sollen durch effektiven IT-Einsatz erreicht werden.“ (www.cio.bund.de)?

20. Welche Personen sind für welche Behörden oder Verbände in dem Nationalen Cyber-Sicherheitsrat vertreten?

21. Treffen Medienmeldungen zu, dass diesem Nationalen Cyber-Sicherheitsrat auch „assoziierte Mitglieder“ der Wirtschaft angehören sollen, und wenn ja, welche Vertreter sollen dies sein, wer wählt oder bestimmt sie, und wem gegenüber sind sie verantwortlich?

22. Welche Aufgaben gehören zur Koordinationstätigkeit des Nationalen Cyber-Sicherheitsrats gegenüber dem Nationalen Cyber-Abwehrzentrum, und ist damit auch eine Art Weisungsbefugnis verbunden?

23. Wie ist die parlamentarische Kontrolle des Nationalen Cyber-Sicherheitsrates und des Nationalen Cyber-Abwehrzentrums geregelt?

24. Treffen Medienmeldungen zu, dass im Falle einer „unmittelbar bevorstehenden oder eingetretenen Krise“ ein nationaler Krisenstab eingerichtet wird, und wenn ja, wie sind die Tätigkeit und die Befugnisse dieses Krisenstabes durch welche Richtlinien geregelt (bitte der Antwort beilegen), welche Personen aus welchen Behörden und Einrichtungen sollen in diesem Krisenstab mitarbeiten, und wie soll die Tätigkeit des Krisenstabes parlamentarisch kontrolliert werden?

25. Wie definiert die Bundesregierung in diesem Zusammenhang eine Situation einer „unmittelbar bevorstehenden Krise“ im Vergleich zu einer „eingetretenen Krise“, und wer ist für die Feststellung der einen und der anderen mit welchen Befugnissen zuständig?

26. Welche Art von Rechenschafts- und Berichtspflichten gibt es für das Nationale Cyber-Abwehrzentrum und den Nationalen Cyber-Sicherheitsrat?

27. Treffen Medienmeldungen zu, dass auch eine Task Force „IT-Sicherheit in der Wirtschaft“ zum 29. März 2011 eingerichtet werden sollte, und wenn ja, nach welchen Richtlinien soll diese Task Force arbeiten (bitte der Antwort beifügen), welche Vertreter welcher Wirtschaftsverbände und welcher Sicherheitsbehörden sollen in dieser Task Force vertreten sein, welche Aufgaben haben sie, wie viele Kosten fallen für diese Task Force an, wird diese Task Force über eine eigene Datei verfügen, und wer soll auf diese Datei zugriff haben?
28. Mit welchen Einrichtungen der EU soll das Nationale Cyber-Abwehrzentrum nach den bisherigen Planungen und Vorgesprächen zusammenarbeiten oder kooperieren?
29. Wann wurde das BMI durch wen beauftragt, eine „Cyber-Außenpolitik (so zu) gestalten, dass deutsche Interessen und Vorstellungen in Bezug auf Cyber-Sicherheit in (…) der NATO koordiniert und gezielt verfolgt werden“ können (Cyber-Sicherheitsstrategie für Deutschland, Hrsg. BMI)?
30. Wann wurde das BMI von wem aufgefordert, die NATO bei der Erarbeitung einheitlicher Sicherheitsstandards zu unterstützen, die dann „freiwillig“ für den Schutz ziviler Kritischer Infrastrukturen übernommen werden sollen (ebd.)?
31. Welche Vorarbeiten zur Entwicklung dieser einheitlichen Sicherheitsstandards wurden bis heute von der NATO geleistet, und inwiefern war das BMI daran beteiligt, bzw. in welcher Form hat sich die Befürwortung des Engagements des BMI gegenüber der NATO gezeigt?
32. Seit wann ist die NATO das „Fundament transatlantischer Sicherheit“ (ebd.) auch im Bereich ziviler Sicherheit und des Schutzes der deutschen bzw. europäischen Kritischen Infrastrukturen?
33. In welcher der beiden Einrichtungen – Nationales Cyber-Abwehrzentrum und Nationaler Cyber-Sicherheitsrat – sollen die einheitlichen NATO-Sicherheitsstandards für ihren zivilen Einsatz geprüft werden, und welche NATO-Vertreter oder -gremien werden daran teilnehmen?
34. Aufgrund welcher Überlegungen, rechtlicher und verfassungsrechtlicher Grundlagen hält es die Bundesregierung für gerechtfertigt, zivile Gremien zu schaffen – Nationales Cyber-Abwehrzentrum und Nationaler Cyber-Sicherheitsrat – an denen Bundeswehr und NATO beteiligt sind und die dem Schutz ziviler Strukturen Standards vorgeben sollen, die für den militärischen Bereich entwickelt wurden?
35. Welche Anstrengungen hat die Bundesregierung bisher unternommen, um für den Schutz Kritischer Infrastrukturen einheitliche zivile Standards zu entwickeln (bitte auch die europäische Ebene beachten)?

Berlin, den 12. April 2011

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333